37th TF-CSIRT meeting
27-28 September 2012
Hotel Slon, Ljubljana, Slovenia.

1. Approval of Minutes

The minutes of the last meeting held on 10 May 2012 were approved.

2. Actions from last meeting

There were no open actions.

3. New TF-CSIRT structure

Kevin Meynell reported on the latest TF-CSIRT developments (see http://www.terena.org/tf-csirt/meeting37/meynell-new-structure.pdf).

The new Terms of Reference (as discussed at the previous meeting) had been approved by TERENA on 14 June 2012 with minor amendments, and took effect from 1 September 2012. These introduced task force membership based on existing TI categories, an elected Chair, and a Steering Committee with an enhanced role. The new Terms of Reference also consolidated the existing ad-hoc procedural documents and could be found at http://www.terena.org/tf-csirt/publications/ToR-2012.pdf

The elections for the Chair and two Steering Committee positions would take place later that day, and separate elections would be held for each position with convention style voting as previously used for the TI Review Board. Potential candidates required two nominations from TF-CSIRT Full Members in order to stand. Each TF-CSIRT member had one vote per round, although if only one candidate is nominated for a particular position, they would be declared elected unopposed.

Kevin then outlined the roles and responsibilities of the Chair and Steering Committee members.

The Chair would be elected for a 2-year term, and could serve a maximum of 2 consecutive terms. They were responsible for leading and representing TF-CSIRT, chairing the Steering Committee, chairing the TF-CSIRT meetings, and determining the agenda of TF-CSIRT meeting in cooperation with the TF-CSIRT Secretary.

The Steering Committee was comprised of the TF-CSIRT Chair, TF-CSIRT Secretary, and 4 elected representatives. The elected representatives served 2-year terms, although these were staggered so that 2 were scheduled to be elected each year. Representatives could serve a maximum of 2 consecutive terms, although could go on to serve an additional term as TF-CSIRT Chair.

A transitional arrangement had been agreed whereby TI Review Board members Przemek Jaroszewski and Wilfried Wöber would continue to serve on the Steering Committee until September 2013. Erika Stockinger's term was already due to finish, although she was

eligible to stand for election again.

The Steering Committee usually met three times per year at TF-CSIRT meetings, although occasionally held additional teleconferences. Its responsibilities were as follows:

- Making decisions on CSIRT accreditation and certification in accordance with the guidelines. This was a responsibility inherited from the TI Review Board.
- Reviewing the performance of the Trusted Introducer service and making recommendations to modify or expand it. This was a responsibility inherited from the TI Review Board.
- Overseeing the development of the TRANSITS training curricula and course materials, monitoring tutoring standards, and registration of tutors.
- Coordinating the activities of TF-CSIRT and recommending courses of action where issues occur.
- Advising on future developments and strategic directions in computer security. This was mostly envisaged with respect to the TF-CSIRT community rather than advising external bodies on behalf of TF-CSIRT.
- Providing input on meeting agendas.

Finally, the new TF-CSIRT logos were shown. These had been modified from those previewed at the previous meeting in response to the feedback received.

Kauto raised a query about the Steering Committee advising on future developments and strategic directions. Kevin replied this was intended to mean advising the TF-CSIRT community, rather than advising external parties. In the past though, the TF-CSIRT Chair and TERENA had occasionally been asked to comment on CSIRT and computer security matters, even though it was always made clear that individual CSIRTs might have different viewpoints. It would therefore be better if elected representatives of the TF-CSIRT community could be consulted in these matters.

Andrew Cormack suggested that 'informed' might be a better term than 'advise'.

Matthew Cook suggested having themed slots during TF-CSIRT meetings. Kevin said this suggestion would be taken on board for future meetings.

4. RU-CERT presentation

Dimitry Ippolitov gave a presentation about RU-CERT (see http://www.terena.org/tf-csirt/meeting37/ippolitov-ru-cert.pdf).

RU-CERT provided an incident prevention and response service for all users located in Russia, with the exception of government facilities that were covered by the government CERT. They also provided assistance in contacting other Russian incident response teams, abuse services and law enforcement agencies.

RU-CERT was sponsored by the Russian Institute for Public Networks (RIPN) which was a non-governmental not-for-profit organisation that coordinated and facilitated access to public networks. The team currently comprised 5 full-time people.

? asked whether RU-CERT had any contact with CERT-GIB. Dimitry replied they knew them, but did not regularly communicate with them.

5. CERT-Bund presentation

Michael Dwucet gave a presentation about CERT-Bund (see http://www.terena.org/tf-csirt/meeting37/dwucet-cert-bund.pdf). It operated under the Federal Office for Information Security and provided incident handling and response services to the German Federal Government, as well as being a CSIRT of last resort. It had been operational since 1994 (originally as BSI-CERT) and currently comprised 15 people.

CERT-Bund aimed to provide incident warning and response services, but also closely collaborated with the National IT Situation Centre that monitored the current state of government networks, and the National IT Crisis Reaction Centre that could respond to serious incidents. They also had a close working relationship with DFN-CERT and various industrial and commercial CSIRTs. In addition, they participated in the CERT Verbund that comprised around 30 other teams.

Serge Droz commented that it had always been difficult to liaise with German CSIRTs because of restrictive data protection laws. He asked whether this situation was likely to be resolved in future.

6. ENISA-CERT relations

Andrea Dufkova reported on the latest ENISA developments.

The ENISA training materials had been extended to include mobile device forensics, investigation of DDoS traces, NetFlow analysis and honeypot deployment. There was also additional material on developing CSIRT infrastructures, establishing external relations, and costing security incidents.

ENISA was also conducting a follow-on study in early warning systems, and in particular whether honeypots were useful for CSIRTs. Are they a practical tool for developing intelligence about threats, and who is undertaking the attacks?

The CERT Inventory Map that displayed all the known CSIRTS in the European Region had been re-designed and updated, whilst the the European Information Sharing and Alert System (EISAS) was being piloted by CESICAT, CertHU, CertPL, NorSIS, Deutsche Telekom and La Caixa.

In addition, the 7th CERT workshop would be held on 16-17 October 2012 in Den Haag, the Netherlands. This would focus on developing cooperation between national/government CERTs and their national law enforcement counterparts.

Andrea then discussed the latest report on baseline capabilities of national and government CSIRTs that would shortly be published. The aim of the study was to define and agree on minimum capabilities for national and government CSIRTs, in order to improve incident response and handling at the national and cross-border level.

National and government CSIRTs had been established in nearly all EU Member States, and have capabilities in line with the recommendations issued by ENISA in 2009. There was a lot of variety in how such CSIRTs were established and hosted, although there was a trend towards creating national cybersecurity centres.

A great deal of work was still needed to properly incorporate such CSIRTs into national cybersecurity strategies, and indeed only 50% of EU member states had national strategies at all. On the positive side though, 90% of national and government CSIRTs were involved in the development of laws and strategies in the area of cybersecurity.

Other concerns were lack of funding and staffing, which led to insufficient specialisation in areas such as forensics, vulnerability handling, legal issues and public relations. There was sometimes also reluctance for commercial constituents to share information for competitive reasons, although informal approaches could still be effective.

Most of the outstanding issues could be defined as political and legal, although as with the rest of the CSIRT community, national and government CSIRTs needed to be willing to respond to new cybersecurity challenges that arose.

Michael Dwucet asked whether ENISA could provide support for developing incident handling software such as RTIR. Andrea said this was not in the current programme, but the programme for 2014 would be agreed this coming November. This should be discussed with representatives of the ENISA Stakeholder Group, of which Andrew Cormack was one.

7. Ransomware Cases

Przemek Jaroszewski reported on some ransomware cases that had recently been seen in Poland.

Otmar Lendl said they had been seeing similar things in Austria, although there seemed to be two different strains of ransomware. Kauto Huopio added the Finnish law enforcement authorities were actually paying attention to this problem due to the financial demands being made, so it was important to communicate cases.

8. Fake Colleges

James Davis gave a presentation about fake college websites that seemed to be springing up in the UK. These were of varying quality, but some appeared to be very professional even though provided postal addresses were other businesses, and telephone numbers were diverted to mobile phones.

It was unclear why these sites were being created and who was doing it. One possibility was an immigration scam in order for people to obtain student visas, but the immigration authorities could easily check institutions against an accredited list so this seemed implausible. Another possibility was for issuing false diplomas, but none of the sites actually appeared to be offering anything like this.

James therefore asked whether anyone else had encountered this, or had any idea of why it was being done.

Serge Droz suggested that someone could pose as a potential student to see where it led. It would probably need to be done from outside the UK to be convincing, but it could be an interesting exercise.

9. X-ARF Developments

Torsten Voss reported on the latest X-ARF developments (see http://www.terena.org/tf-csirt/meeting37/voss-x-arf.pdf).

They wished to add optional end-to-end security for X-ARF messages either using S/MIME or PGP/MIME. In order to maintain backwards compatibility, the plan was to use 'X-XARF:

PLAIN' or 'X-XARF: SECURE' in the mail header to indicate the use of X-ARF v0.2 and that the RFC822 container is signed and/or encrypted. That would allow existing importers and exporters to handle legacy X-ARF messages without change.

10. Report on Academic CSIRT workshop

Kevin Meynell gave a short report on the second Academic CSIRT workshop (see http://www.terena.org/tf-csirt/meeting37/meynell-academic-csirts.pdf).

This was a one-day meeting organised on 17 June 2012 at FIRST 24 in Malta, and involved 22 academic CSIRTs from Europe, Asia and Latin America. The aim was to discuss particular issues affecting CSIRTs serving NRENs and R&E institutions. Presentations can be found at http://www.terena.org/tf-csirt/academic-meeting-2/

RedCLARA, the Latin American R&E network, had established a working group of NREN CSIRTs known as GT-CSIRT. This coordinated by Nina Solha (RNP) and covered 15 countries in Latin America. Its activities included malicious activity monitoring (using the SurfIDS tool), security incident monitoring (using Shadowserver, zone-h and Spamcop), encouraging the establishment of new CSIRTs along with training, and development of a web-based contacts and incidents manager.

There was also a proposal to establish an Academic CSIRT Special Interest Group within FIRST. This was being followed-up by Margrete Raaum (UiO-CERT & FIRST).

11. Election of TF-CSIRT officials

Lionel Ferette was the only nominated candidate for Chair, so was declared unelected unopposed for a 2-year term.

There were three nominated candidates for the two Steering Committee positions, so two elections were necessary:

Position No. 1

1st round - Kauto Huopio, 16 votes; Erika Stockinger, 13 votes; Jacques Schuurman, 12 votes (eliminated)

2nd round – Erika Stockinger, 22 votes (elected); Kauto Huopio, 21 votes

Position No. 2

1st round – Jacques Schuurman, 25 votes (elected); Kauto Huopio, 18 votes

Erika Stockinger (CERT-SE) and Jacques Schuurman (XS4ALL) were therefore elected for a 2-year term each.

12. Examining incident handling procedures

Otmar Lendl gave a presentation about incident handling procedures.

13. Squaring the Circle: Reflections on Identities, AuthN & AuthZ at CERN

Stefan Lüders gave a presentation on two-factor authentication at CERN (see http://www.terena.org/tf-csirt/meeting37/lueders-identities.pdf).

This was motivated by the traditional lack of control over users and accounts at CERN which experienced a high turnover of staff who tended to have an open and collaborative mindset. It was relatively easy to obtain an account at CERN, and this resulted in a multitude of accounts and websites that were all using CERN computing resources even once the users moved on (or were never actually associated with CERN in the first place).

The plan was therefore to introduce a single sign-on portal for all computing services, which would also allow proper authentication mechanisms and authorisation to be undertaken. Beyond this, the idea was to utilise identity federations so that CERN users could use accounts from their home institutions. However, the more identity federations that were joined, the more complexity, so trust networks like IGTF ultimately needed to considered. This was currently under discussion at the Federated Identity Management (FIM) Workshops.

14. Catering for Increased Network Capacities in Anomaly Detection Tools

Juan Quintanilla gave a presentation on the NSHaRP service (see http://www.terena.org/tf-csirt/meeting37/quintanilla-anomaly-detection.pdf). This was based on Netreflex 2.5, Nfsen and Splunk and provided an automated anomaly detection and alerting system for the GÉANT network.

The forthcoming GÉANT Plus network would bring some new challenges though, as it would move to 100 Gb/s circuits and would converge the production IP and bandwidth-on-demand provisioning layers. In addition, the GÉANT Lambda services (point-to-point 10 Gb/s lightpaths) may need to be supported.

This meant more hardware capacity was required, as well as software that could cope with the increased bitrates and number of flows. NetReflex 2.9 was therefore being rolled out in a staged migration, and approximately three-quarters of the nodes had been upgraded to-date.

15. CERT.LV collaborations with ISPs, security professionals and ordinary people

Baiba gave a presentation on the CERT.LV efforts to develop relationships with the Latvian IT community (http://www.terena.org/tf-csirt/meeting37/kaskina-user-collaborations.pdf).

Under a Latvian IT Security law, all ISPs were expected to submit an action plan for continuous operations to CERT.LV, report all major incidents, and CERT.LV could request security documentation, undertake security audits, and even disconnect users if necessary. There were more than 400 ISPs in Latvia though, most of which served very small communities, so in reality persuasion and building good relationships was more productive. As a result, they had created some model action plans that could be adopted by ISPs, and had introduced a 'Responsible ISP' scheme whereby ISPs signing an MoU agreeing to uphold certain principles could display a 'Responsible ISP' logo.

The LV CSIRT group had been established in 2007 with the aim of exchanging contact details and experience, but it suffered from inactivity and a lack of trust. However, the concerns of the Latvian government and the establishment of the Estonian Cybersecurity

League led to the establishment of the Security Expert Group under the auspices of CERT.LV which had monthly meetings, and rules on who was able to participate. A Latvian Cybersecurity League had also been formed by the Ministry of Defence, which currently had 25 members.

Another idea was the introduction of the 'Computerologist' whereby CERT.LV staff would go to public events to provide security advice to end users, as well as scan computers to check for malware. The first event had been held on 12 May, and whilst it was quite a labour intensive effort, there were plans to repeat this exercise.

16. Malware repositories, a need for CERTs

Steve Clement gave a presentation on the malware.lu respository (see http://www.terena.org/tf-csirt/meeting37/clement-malwarerepo.pdf).

This had been created by Paul Rascagneres and was maintained by him and Hugo Caron in order to provide a common malware repository for the CSIRT community. It presently contained over 3 million samples for forensic analysis, reverse engineering, building tools for detection and analysis, and other security research. Access was via web interface or HTTP REST API and restricted to registered users. Users could search on a specific hash, download malware, and upload samples.

The Hack.lu workshop that was being held on 23-25 October 2012 in Luxembourg was also announced.

17. Discussion on TF-CSIRT activities

Lionel Ferette said the Task Force had to review its current list of activities (see (http://www.terena.org/tf-csirt/meeting37/ferette-activities.pdf). Under the new Terms of Reference, these would now be reviewed annually instead of upon re-chartering (which was approximately every two years). In addition, Trusted Introducer and TRANSITS are now considered permanent services of the task force, so neither needed to be explicitly included on the list.

Kevin Meynell added that a definitive list of activities did not need to be produced at this meeting, and it would be better to align this with the calendar year. This meeting should therefore be used to kick-off the discussion, with a view to finalising a plan for 2013.

Of the other activities on the list, RTIR developments were being discussed and there was a proposal to revive the RTIR Working Group. This activity should therefore continue, and perhaps other incident handling tools could be investigated as well.

With respect to the Abuse Contacts activity, it seemed around 20 teams currently maintained the IRT object in the RIPE database. However, with the recent RIPE proposals to deprecate this, this activity no longer seemed relevant.

The Clearing House of Incident Handling Tools (CHIHT) was hosted at ENISA and described as a collaboration with TF-CSIRT. However, it was unclear how actively this was maintained by the TF-CSIRT community. Andrea Dufkova said she'd ask Marco Thorbrugge about current status.

Action 37.1 – Andrea Dufkova to ask Marco Thorbrugge about the current status of CHIHT.

TF-CSIRT already had active liaisons with FIRST, ENISA and AP-CERT, and had recently developed a liaison with OAS-CICTE. However, perhaps more active liaisons could be developed with other regional CSIRT bodies (e.g. GT-CSIRT).

Jan Vykopal (?) suggested creating a working group on NetFlow tools to share methods and techniques. Kauto Huopio also suggested investigating the further deployment of XMPP, whilst the presentation by Steve Clement earlier in the meeting had led to further discussion on the development of malware repositories.

Lionel said that he would continue the discussion on the mailing list, as well as solicit other ideas.

Action 37.2 – Lionel Ferette to continue discussion about TF-CSIRT activities on the mailing list.

18. Date of next meeting

Lionel Ferette thanked SI-CERT for hosting the meeting.

The next meeting will be held on 28-29 January in Lisbon, Portugal (hosted by FIRST and FCCN). This would be in conjunction with the FIRST Technical Colloquium.

Open Actions

37.1 Andrea Dufkova to ask Marco Thorbrugge about the current status of CHIHT.

37.2 Lionel Ferette to continue discussion about TF-CSIRT activities on the mailing list.

Participants

Name	*Organisation*	*Country*
Hillar Aareleid	CERT-EE	Estonia
Shehzad Ahmad	DK-CERT (UNI-C)	Denmark
Claudio Allocchio	GARR	Italy
Mateo Araque	CCN-CERT	Spain
Mihai Barbulescu	RoCSIRT	Romania
Johan Berggren	NORDUnet	-
Wim Biemolt	SURFcert (SURFnet)	The Netherlands
Vladimir Bobor	TS-CERT	Sweden
Gorazd Božič	SI-CERT	Slovenia
Matej Breznik	SI-CERT	Slovenia
Steve Clement	CIRCL	Luxembourg
Ian Cook	Team Cymru	United Kingdom
Matthew Cook	Loughborough University/ESISS	United Kingdom
James Davis	Janet CSIRT	United Kingdom
Serge Droz	SWITCH	Switzerland
Andrea Dufkova	ENISA	-
Jacqueline Dulmaine	CERT.be	Belgium
Michael Dwucet	CERT-Bund	Germany
Øyvind Eilertsen	UNINETT CERT	Norway
Torsten Enquist	TS-CERT	Sweden
Lionel Ferette (Chair)	-	Belgium
Guy Foetz	GOVCERT.LU	Luxembourg
Martin Hathaway	BT CERT	United Kingdom
Lukas Hlavicka	CSIRT.SK	Slovakia
Patrick Houtsch	GOVCERT.LU	Luxembourg
Tadej Hren	SI-CERT	Slovenia
Kauto Huopio	CERT-FI (FICORA)	Finland
Dimitry Ippolitov	RU-CERT	Russia
Przemek Jaroszewski	CERT Polska (NASK)	Poland
Jonas Juknius	CERT-LT	Lithuania
Bob van der Kamp	NCSC-NL	The Netherlands
Baiba Kaskina	CERT.LV	Latvia
Peter Kijewski	CERT Polska (NASK)	Poland
Andrea Kropacova	CESNET CERTS	Czech Republic
Otmar Lendl	CERT.at	Austria
Antonio Liu	Trusted Introducer	Germany
Stefan Lueders	CERN	-
Mirek Maj	Cybersecurity Foundation	Poland
Godert Jan van Maren	NCSC-NL	The Netherlands
Branko Mažar	CARNet	Croatia
Kevin Meynell (Secretary)	TERENA	-
Jasmina Mešić	SI-CERT	Slovenia
Dave Monnier	Team Cymru	United States
Francisco Monserrat	IRIS-CERT (RedIRIS)	Spain
Rolf Sture Normann	UNINETT	Norway
Tomas Nowocien	Pionier-CERT	Poland
Leila Pohjolainen	Funet CERT	Finland
Timo Porjamo	Funet CERT	Finland
Wayne Routly	DANTE	-
Martin Schroeter	SWITCH	Switzerland
Jacques Schuurman	XS4ALL	The Netherlands
Kristian Selén	CERT-FI (FICORA)	Finland
Adam Smutnicki	WCNS/EGI-CSIRT	Poland

Marc Stiefer	RESTENA-CSIRT	Luxembourg
Erika Stockinger	CERT-SE	Sweden
Manuel Subredu	RoCSIRT	Romania
Alexey Sukhikh	RU-CERT	Russia
Alexander Talos-Zens	ACOnet-CERT	Austria
Marius Urkis	LITNET CERT	Lithuania
Jeroen Vanderauwera	CERT.be	Belgium
Dimitra Vitsa	FORTHcert	Greece
Torsten Voss	DFN-CERT	Germany
Jan Vykopal	CSIRT-MU	Czech Republic
Cynthia Wagner	RESTENA	Luxembourg
Jagor Čakmak	CARNet	Croatia

Apologies were received from:

Alexandre Dulaunoy	CIRCL	Luxembourg
Vincent Hinderer	CERT-LEXSI	France
Klaus-Peter Kossakowski	PRESECURE	Germany
Tural Mammadov	CERT.GOV.AZ	Azerbaijan
Margrete Raaum	UiO-CERT	Norway
Don Stikvoort	S-CURE	The Netherlands
Pascal Steichen	CIRCL	Luxembourg
Thomas Stridh	SUNet CERT	Sweden
Marco Thorbruegge	ENISA	-
Mirko Wollenberg	PRESECURE	Germany
Wilfried Wöber	ACOnet-CERT	Austria